IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:	Confirmation Number: 5515
Yik, *et al.*	Group Art Unit: 2434
Serial No.: 09/866,259	Examiner: Tolentino, Roderick
Filed: May 25, 2001	Docket No.: 250338-1470

For: Data Network Mode Having Enhanced Security Features

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief under 37 C.F.R. § 41.37 is submitted in support of the Notice of Appeal filed May 20, 2009, responding to the Final Office Action mailed February 25, 2009.

It is not believed that extensions of time or fees are required to consider this Appeal Brief. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required are hereby authorized to be charged to Deposit Account No. 50-0835.

I. Real Party in Interest

The real party in interest is Conexant Systems, Inc. having a place of business at 4000 MacArthur Blvd., Newport Beach CA, 92660.

II. Related Appeals and Interferences

There are no known related appeals or interferences that will affect or be affected by a decision in this Appeal.

III. Status of Claims

Claims 1 – 20 stand finally rejected. No claims have been allowed. The final rejections of claims 1 – 20 are appealed.

IV. Status of Amendments

No amendments have been made or requested since the mailing of the Final Office Action and all amendments submitted prior to the Final Office Action have been entered. The claims in the attached Claims Appendix (see below) reflect the present state of the pending claims.

V. Summary of Claimed Subject Matter

The claimed subject matter is summarized below with reference numerals and references to the written description ("specification") and drawings. The subject matter described in the following appears in the original disclosure at least where indicated, and may further appear in other places within the original disclosure.

Embodiments according to independent claim 1 describe a "secure data switching node (page 7, line 11 and FIG. 1, element 100) comprising: a plurality of communications ports (page 7, line 18 and FIG. 1, element 106); a switching database

(page 7, line 12 and FIG. 1, element 102) having a plurality of switching entries (page 8, lines 10 and 14 and FIG. 2, element 202), each one of the plurality of switching entries specifying an association between one or more data network node identifiers and one or more respective communications ports (FIG. 1, element 106); a plurality of switching entry protection flags (page 8, line 17 and FIG. 2), corresponding to the plurality of switching entries, each of the plurality of switching entry protection flags configured with a predetermined value that determines whether each of the switching entries is protected from update (page 9, line 1 and FIG. 2); and a controller executing a secure switching database update process, for at least one of the switching entries (page 7, line 12 and FIG. 1, element 101), wherein executing a secure switching database update process includes determining, from at least one of the switching entry protection flags (page 8, line 17 and FIG. 2), whether the at least one of the switching entries is protected from update (page 9, line 8) and receiving a modification instruction including a change of at least one of the respective communications ports (FIG. 1, element 106) for at least one of the data network node identifiers (page 9, line 15), whereby an attempt by a hostile data network node to effect a modification of the at least one communication port of a protected switching entry is prevented when the protection flag is set (page 9, line 12), enabling the data switching node to operate securely concurrently in friendly and hostile data networking environments."

Embodiments according to independent claim 3 describe a "secure data switching node (page 7, line 11 and FIG. 1, element 100) comprising: a. a plurality of physical communications ports (page 7, line 18 and FIG. 1, element 106); a switching database (page 7, line 12 and FIG. 1, element 102) having a plurality of switching entries (page 8, lines 10 and 14 and FIG. 2, element 202), each one of the plurality of switching entries specifying an association between one or more data network node identifiers and one or more of the respective physical communications ports (page 8, line 17 and FIG.

2); a plurality of topology discovery disable flags corresponding to the plurality of switching entries, each of the plurality of topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database (page 11, line 7 and FIG. 3); and a controller executing a secure data transport network topology update process for at least one of the switching entries (page 7, line 12 and FIG. 1, element 101), wherein executing a secure data transport network topology update includes determining, from at least one of the topology discovery disable flags (page 11, line 6 and FIG. 3), whether switching entries are prevented from being added to the switching database (page 11, line 6) and receiving an addition instruction including a change of at least one of the respective communications ports (FIG. 1, element 106) for at least one of the data network node identifiers (page 11, line 14), whereby attempts by a hostile data network node to effect at least one addition of a switching entry specifying a communications port (FIG. 1, element 106) associated with a topology discovery disabled physical communications port (FIG. 1, element 106) are prevented, enabling the data switching node to operate securely concurrently in friendly and hostile data networking environments (page 11, line 14).

Embodiments according to independent claim 4 describe a "secure data switching node (page 7, line 11 and FIG. 1, element 100) comprising: a plurality of physical communications ports (page 7, line 18 and FIG. 1, element 106); a switching database (page 7, line 12 and FIG. 1, element 102) having a plurality of switching entries (page 8, lines 10 and 14 and FIG. 2, element 202), each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port (page 8, line 17 and FIG. 2); a plurality of topology discovery disable flags (page 11, line 7 and FIG. 3), corresponding to the plurality of switching entries, each of the plurality of topology discovery disable flags configured with a

predetermined value that determines whether additional switching entries are prevented from being added to the switching database; a global unknown destination flood control flag; and a controller (page 7, line 12 and FIG. 1, element 101) implementing a secure Payload Data Unit (PDU) forwarding process (page 13, line 10 and FIG. 5), the PDU forwarding process including a modification instruction (page 9, line 15) including a change of at least one communication port for at least one of the data network node identifiers, a received PDU having a destination data node identifier not stored in the switching database (page 7, line 12 and FIG. 1, element 102) is replicated only to physical communications ports (FIG. 1, element 106) having reset topology discovery disable flags preventing hostile data network nodes connected thereto from listening to unknown destination data traffic (page 12, line 6), wherein implementing a secure Payload Data Unit (PDU) forwarding process includes determining, from at least one of the topology discovery disable flags, whether switching entries are prevented from being added to the switching database (page 13, line 27 and FIG. 5, element 510).

Embodiments according to independent claim 5 describe a "secure data switching node (page 7, line 11 and FIG. 1, element 100) comprising: a plurality of physical communications ports (page 7, line 18 and FIG. 1, element 106); a switching database (page 7, line 12 and FIG. 1, element 102) having a plurality of switching entries (page 8, lines 10 and 14 and FIG. 2, element 202), each one of the plurality of switching entries (page 8, lines 10 and 14 and FIG. 2, element 202) specifying an association between at least one data network node identifier and at least one of the communications ports (FIG. 1, element 106); a plurality of unknown destination flood control flags (page 11, line 28), corresponding to the plurality of switching entries (page 8, lines 10 and 14 and FIG. 2, element 202), each of the plurality of unknown destination flood control flags configured with a predetermined value that determines whether replication of Payload Data Unit (PDU) to communication ports is prevented; and a

controller implementing a secure Payload Data Unit (PDU) forwarding process, wherein implementing a secure Payload Data Unit (PDU) forwarding process includes determining, from at least one of the unknown destination flood control flags, whether replication of PDU to communication ports is prevented (page 12, line 6), the PDU forwarding process further including receiving a modification instruction including a change of at least one of the communication ports for at least one of the data network node identifiers (page 9, line 15), whereby a received PDU having as a destination data node identifier not stored in the switching database (FIG. 1, element 102) is replicated only to physical communications ports (FIG. 1, element 106) having reset unknown destination flood control flags preventing hostile data network nodes connected thereto from listening to unknown destination data traffic (page 12, line 6).

Embodiments according to independent claim 6 describe a "method of securely updating a switching database (FIG. 1, element 102) of a data switching node (FIG. 1, element 100) forwarding data traffic in a data transport network, the method comprising steps of: extracting a source data network node identifier from data traffic received on a source physical communications port (FIG. 1, element 106) of the data switching node (page 13, line 14); querying the switching database (page 11, line 7 and FIG. 1, element 102) having a plurality of switching entries (page 8, lines 10 and 14 and FIG. 2, element 202), each one of the plurality of switching entries (page 8, lines 10 and 14 and FIG. 2, element 202) specifying an association between a data network node identifier and a communications port (page 8, line 18 and FIG. 2), the query using the extracted source data network identifier as a key, the switching database including a field for indicating a predetermined value associated with the source data network node identifier configured to indicate whether a new switching entry is prevented from being added to the switching database (page 11, line 1 and FIG. 3); receiving a modification instruction including a change of the communication port for the data network node identifier (page 9, line 15);

adding a new switching entry to the switching database if a switching entry corresponding to the source data network node identifier does not prevent entry to the switching database (page 12, line 16); and modifying the communications port (FIG. 1, element 106) specification of a switching entry found to correspond to the extracted source data network node identifier (page 13, line 27), if a switching entry protection flag associated with the found switching entry is reset whereby preventing a redirection of data traffic processed by the data switching node.

Embodiments according to independent claim 7 describe a "method of securely updating data transport network topology information held in a switching database (FIG. 1, element 102) of a data switching node (FIG. 1, element 100) associated with the data transport network, the method comprising steps of: extracting a source data network node identifier from data traffic received on a source physical communications port (FIG. 1, element 106) of the data switching node (page 13, line 14); querying the switching database having a plurality of switching entries, each one of the plurality of switching entries (page 8, lines 10 and 14 and FIG. 2, element 202) specifying an association between a data network node identifier and a communications port (page 11, line 7 and FIG. 1, element 102), the query using the extracted source data network node identifier as a key, the switching database (FIG. 1, element 102) including a field for indicating a predetermined value associated with a topology discovery disable flag configured to indicate whether switching entries are prevented from being added to the switching database (page 11, line 1 and FIG. 3); and receiving a modification instruction including a change of the communication port for the data network node identifier (page 9, line 15); adding a new switching entry to the switching database (FIG. 1, element 102) if a switching entry corresponding to the source data network node identifier is not found in the switching database and the topology discovery disable flag is reset whereby a hostile

data network node is prevented from connecting to the source physical communications port (page 12, line 16).

Embodiments according to independent claim 10 describe a "secure method of forwarding data traffic having a destination unknown to a data switching node (FIG 1, element 100), the method comprising steps of: extracting a source data network node identifier from the unknown destination data traffic received on a source physical communications port (FIG. 1, element 106) of the data switching node (page 11, line 1 and FIG. 3); querying the switching database having a plurality of switching entries each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port (FIG. 1, element 106), the query using the extracted source data network node identifier as a key, the switching database including a field for indicating a predetermined value associated with a global unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented (page 11, line 1 and FIG. 3); receiving a modification instruction including a change of the communication port for the data network node identifier (page 9, line 15); replicating the received data traffic to each one of a plurality of physical communications ports (FIG. 1, element 106) of the data switching node if the global unknown destination flood control flag associated with the data switching node is reset (page 12, line 6); and replicating the received data traffic to each one of the plurality of physical communications ports (FIG. 1, element 106) except physical communications ports (FIG. 1, element 106) having a topology discovery disable feature set if the global unknown destination flood control flag is set whereby a hostile data network node connected to a physical communications port (FIG. 1, element 106) having the topology discovery disable flag set is prevented from spying on unknown destination data traffic (page 12, line 6).

Embodiments according to independent claim 13 describe a "secure method of forwarding data traffic having a destination unknown to a data switching node, the method comprising steps of: a. extracting a source data network node identifier from the unknown destination data traffic received on a source physical communications port (FIG. 1, element 106) of the data switching node (page 11, line 1 and FIG. 3); querying the switching database having a plurality of switching entries each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port (FIG. 1, element 106), the query using the extracted source data network node identifier as a key, the switching database including a field for indicating a predetermined value associated with an unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented (page 11, line 1 and FIG. 3); receiving a modification instruction including a change of the communication port for the data network node identifier (page 9, line 15); replicating the received data traffic to each one of a plurality of communications ports (FIG. 1, element 106) of the data switching node (FIG. 1, element 100) if the unknown destination flood control flags associated with the physical communications ports are reset (page 12, line 6); and replicating the received data traffic to each one of the plurality of physical communications ports except physical communications ports (FIG. 1, element 106) having the unknown destination flood control flag set (page 12, line 6), whereby a hostile data network node connected to a physical communications port having the associated topology discovery disable flag set is prevented from spying on unknown destination data traffic (page 12, line 6).

VI. Grounds of Rejection to be Reviewed on Appeal

The following grounds of rejections are to be reviewed on appeal:

Claims 1, 3 – 7, and 10 – 14 stand rejected under 35 U.S.C. §102(e) as allegedly being unpatentable over U.S. Publication Number 2002/0156888 ("*Lee*").

Claim 2 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Publication Number 2002/0156888 ("*Lee*") in view of U.S. Patent Number 5,996,021 ("*Civanlar*").

Claims 8 and 9 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Publication Number 2002/0156888 ("*Lee*") in view of U.S. Patent Number 4,893,340 ("*Lubarsky*").

Claims 15 – 20 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Publication Number 2002/0156888 ("*Lee*") in view of U.S. Patent Number 7,065,644 ("*Danielf*").

VII. Arguments

Appellant respectfully submits that pending claims 1 – 20 are patentable under 35 U.S.C. §103. Appellant respectfully requests that the Board of Patent Appeals overturn the final rejection of those claims at least for the reasons discussed below.

A. Cited References

1. The *Lee* Reference

Lee discloses a "method of automating the verification of a fabric for interconnecting a cluster of end nodes" (Abstract).

2. The *Civanlar* Reference

Civanlar discloses an "internetwork relay system and method for transmitting IP traffic including an edge and a core" (Abstract).

3. The *Lubarsky* Reference

Lubarsky discloses an "adaptive multijunction unit apparatus for multiplexing data streams between a master computer and a plurality of slave computers coupled through telephone system communication lines" (Abstract).

4. The *Daniell* Reference

Daniell discloses a "security application protects a security profile of a computer system by detecting security settings of the computer system have changed" (Abstract).

B. Rejections Under 35 U.S.C. §102

1. Claim 1 is Allowable Over *Lee*

The Office Action indicates that claim 1 stands rejected under 35 U.S.C. §102(e) as allegedly being anticipated by U.S. Patent Publication Number 2002/0156888 ("*Lee*"). Appellant respectfully traverses this rejection on the grounds that *Lee* does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 1 recites:

A secure data switching node comprising:

a. a plurality of communications ports;

b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between one or more data network node identifiers and one or more respective communications ports;

c. ***a plurality of switching entry protection flags, corresponding to the plurality of switching entries, each of the plurality of switching entry protection flags configured with a predetermined value that determines whether each of the switching entries is protected from update***; and

d. a controller executing a secure switching database update process, for at least one of the switching entries, wherein executing a secure switching database update process includes ***determining, from at least one of the switching entry protection flags, whether the at least one of the switching entries is protected from update*** and receiving a modification instruction including a change of at least one of the respective communications ports for at least one of the data network node identifiers, whereby an attempt by a hostile data network node to effect a modification of the at least one communication port of a protected switching entry is prevented when the protection flag is set, enabling the data switching node to operate securely concurrently in friendly and hostile data networking environments.

(Emphasis added).

Appellant respectfully submits that claim 1 is allowable for a least the reason that *Lee* fails to disclose, teach, or suggest a "secure data switching node comprising... ***a plurality of switching entry protection flags, corresponding to the plurality of switching entries, each of the plurality of switching entry protection flags configured with a predetermined value that determines whether each of the switching entries is protected from update***... [and] ***determining, from at least one of the switching entry protection flags, whether the at least one of the switching entries is protected from update***" as recited in claim 1. First, *Lee* was filed December 21, 2001, which is after the May 25, 2001 filing date of the present application. Consequently, *Lee* is not prior art without reliance on an earlier filed provisional application.

Second, if the Office Action is attempting to rely on the April 23, 2001 filing date of the *Lee* provisional application (60/285,936), the Examiner must show that the *Lee* provisional application fully supports the claimed subject matter asserted in the rejection. Appellant respectfully submits that the *Lee Provisional* fails to provide support for at least the highlighted features of claim 1. More specifically, the *Lee Provisional* discloses "[e]ach port has a special flag indicating whether the port is 'enabled' (versus disabled) for data transfer" (page 9, last paragraph). As illustrated in this passage, the *Lee Provisional* discloses a flag that indicates whether a port is enabled for data transfer. This is completely different than "***determining, from at least one of the switching entry protection flags, whether the at least one of the switching entries is protected from update***" as recited in claim 1 for at least the reason that indicating whether a port is enabled is different than determining whether a switching entry is protected from update.

Further, the only other somewhat relevant discussion in the *Lee* provisional application discloses "there exists a flag for each port about the validity of the Port Neighbor Information data" (page 13, paragraph "a"). As illustrated in this passage, the *Lee Provisional* discloses a flag regarding validity of information. This is completely different than "***switching entry protection flags configured with a predetermined value that determines whether each of the switching entries is protected from update***" as recited in claim 1. While the Final Office Action argues:

> [The *Lee Provisional*] teaches a flag enabling a port. The port can either be enabled or disabled and this is indicated by a flag, this flag similar to the flag of the claim language in Claim 1 where switching entry protection flags configured with a predetermined value that determines whether each of the switching entries is protected from update. The argument that the Provisional fails to teach an update is moot since updating information via a port is just intended use. Intended use is not patentable material. The port as taught in the provisional shows how the port can transfer data or not based on the flag indicator of the

> port. One of ordinary skill in the art would see how this reads on the claim language in Claim 1 of "protection flags configured with a predetermined value that determines whether each of the switching entries is protected from update.
>
> (FOA page 3, line 15).

Appellant respectfully disagrees. More specifically, the *Lee Provisional* does not disclose the exact same flags that could be used in a manner consistent with claim 1. To the contrary, claim 1 clearly recites "***switching entry protection flags configured with a predetermined value that determines whether each of the switching entries is protected from update***." The switching entry protection flags include different information (*e.g.*, "a predetermined value...") than a flag that simply enables or disables a port, as disclosed in the *Lee Provisional*. Consequently, this is not just "intended use" as argued in the Final Office Action.

For at least the reason that the *Lee Provisional* fails to support a rejection under 35 U.S.C. §102, the rejection is deficient and claim 1 is allowable. As clearly illustrated above, the *Lee* provisional application fails to provide adequate support to substantiate a filing date that would permit *Lee* to be used as a 35 U.S.C. §102(e) reference in rejecting the present application. For at least this reason, claim 1 is allowable.

2. Claim 3 is Allowable Over *Lee*

The Office Action indicates that claim 3 stands rejected under 35 U.S.C. §102(e) as allegedly being anticipated by U.S. Patent Publication Number 2002/0156888 ("*Lee*"). Appellant respectfully traverses this rejection on the grounds that *Lee* does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 3 recites:

A secure data switching node comprising:

a. a plurality of physical communications ports;

b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between one or more data network node identifiers and one or more of the respective physical communications ports;

c. ***a plurality of topology discovery disable flags corresponding to the plurality of switching entries, each of the plurality of topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database***; and

d. a controller executing a secure data transport network topology update process for at least one of the switching entries, wherein executing a secure data transport network topology update includes ***determining, from at least one of the topology discovery disable flags, whether switching entries are prevented from being added to the switching database*** and receiving an addition instruction including a change of at least one of the respective communications ports for at least one of the data network node identifiers, whereby attempts by a hostile data network node to effect at least one addition of a switching entry specifying a communications port associated with a topology discovery disabled physical communications port are prevented, enabling the data switching node to operate securely concurrently in friendly and hostile data networking environments.

(Emphasis added).

Appellant respectfully submits that claim 3 is allowable for a least the reason that *Lee* fails to disclose, teach, or suggest a "secure data switching node comprising… ***a plurality of topology discovery disable flags corresponding to the plurality of switching entries, each of the plurality of topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database***… [and] a controller… ***determining, from at least one of the topology discovery disable flags, whether switching entries are prevented from being added to the switching database***" as recited in claim 3. First, *Lee* was filed December 21, 2001, which is after

the May 25, 2001 filing date of the present application. Consequently, *Lee* is not prior art without reliance on an earlier filed provisional application.

Second, if the Office Action is attempting to rely on the April 23, 2001 filing date of the *Lee* provisional application (60/285,936), the Examiner must show that the *Lee* provisional application fully supports the claimed subject matter asserted in the rejection. Appellant respectfully submits that the *Lee Provisional* fails to provide support for at least the highlighted features of claim 3. More specifically, the *Lee Provisional* discloses "[e]ach port has a special flag indicating whether the port is 'enabled' (versus disabled) for data transfer" (page 9, last paragraph). As illustrated in this passage, the *Lee Provisional* discloses a flag that indicates whether a port is enabled for data transfer. This is completely different than "***determining, from at least one of the topology discovery disable flags, whether switching entries are prevented from being added to the switching database***" as recited in claim 3 for at least the reason that indicating whether a port is enabled is different than determining whether a switching entry is protected from update.

Further, the only other somewhat relevant discussion in the *Lee* provisional application discloses "there exists a flag for each port about the validity of the Port Neighbor Information data" (page 13, paragraph "a"). As illustrated in this passage, the *Lee Provisional* discloses a flag regarding validity of information. This is completely different than "***topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database***" as recited in claim 3. While the Final Office Action argues:

> [The *Lee Provisional*] teaches a flag enabling a port. The port can either be enabled or disabled and this is indicated by a flag, this flag similar to the flag of the claim language in Claim 3 where switching entry protection flags configured with a predetermined value that determines

> whether each of the switching entries is protected from update. The argument that the Provisional fails to teach an update is moot since updating information via a port is just intended use. Intended use is not patentable material. The port as taught in the provisional shows how the port can transfer data or not based on the flag indicator of the port. One of ordinary skill in the art would see how this reads on the claim language in Claim 3 of "protection flags configured with a predetermined value that determines whether each of the switching entries is protected from update.

(FOA page 3, line 15).

Appellant respectfully disagrees. More specifically, the *Lee Provisional* does not disclose the exact same flags that could be used in a manner consistent with claim 3. To the contrary, claim 3 clearly recites "***topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database***." The switching entry protection flags include different information (*e.g.*, "a predetermined value…") than a flag that simply enables or disables a port, as disclosed in the *Lee Provisional*. Consequently, this is not just "intended use" as argued in the Final Office Action.

For at least the reason that the *Lee Provisional* fails to support a rejection under 35 U.S.C. §102, the rejection is deficient and claim 3 is allowable. As clearly illustrated above, the *Lee* provisional application fails to provide adequate support to substantiate a filing date that would permit *Lee* to be used as a 35 U.S.C. §102(e) reference in rejecting the present application. For at least this reason, claim 3 is allowable.

3. Claim 4 is Allowable Over *Lee*

The Office Action indicates that claim 4 stands rejected under 35 U.S.C. §102(e) as allegedly being anticipated by U.S. Patent Publication Number 2002/0156888 ("*Lee*"). Appellant respectfully traverses this rejection on the grounds that *Lee* does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 4 recites:

A secure data switching node comprising:

a. a plurality of physical communications ports;

b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port;

c. ***a plurality of topology discovery disable flags, corresponding to the plurality of switching entries, each of the plurality of topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database***;

d. ***a global unknown destination flood control flag***; and

e. a controller implementing a secure Payload Data Unit (PDU) forwarding process, the PDU forwarding process including a modification instruction including a change of at least one communication port for at least one of the data network node identifiers, a received PDU having a destination data node identifier not stored in the switching database is replicated only to physical communications ports having reset topology discovery disable flags preventing hostile data network nodes connected thereto from listening to unknown destination data traffic, wherein implementing a secure Payload Data Unit (PDU) forwarding process includes ***determining, from at least one of the topology discovery disable flags, whether switching entries are prevented from being added to the switching database***.

(Emphasis added).

Appellant respectfully submits that claim 4 is allowable for a least the reason that *Lee* fails to disclose, teach, or suggest a "secure data switching node comprising… ***a plurality of topology discovery disable flags, corresponding to the plurality of switching entries, each of the plurality of topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database… a global unknown destination flood control flag…*** [and] a controller… ***determining, from at least one of the topology discovery disable flags, whether switching entries are prevented from being added to the switching database***" as recited in claim 4. First, *Lee* was filed December 21, 2001, which is after the May 25, 2001 filing

date of the present application. Consequently, *Lee* is not prior art without reliance on an earlier filed provisional application.

Second, if the Office Action is attempting to rely on the April 23, 2001 filing date of the *Lee* provisional application (60/285,936), the Examiner must show that the *Lee* provisional application fully supports the claimed subject matter asserted in the rejection. Appellant respectfully submits that the *Lee Provisional* fails to provide support for at least the highlighted features of claim 4. More specifically, the *Lee Provisional* discloses "[e]ach port has a special flag indicating whether the port is 'enabled' (versus disabled) for data transfer" (page 9, last paragraph). As illustrated in this passage, the *Lee Provisional* discloses a flag that indicates whether a port is enabled for data transfer. This is completely different than "***determining, from at least one of the topology discovery disable flags, whether switching entries are prevented from being added to the switching database***" as recited in claim 4 for at least the reason that indicating whether a port is enabled is different than determining whether a switching entry is prevented from being added to a database.

Further, the only other somewhat relevant discussion in the *Lee* provisional application discloses "there exists a flag for each port about the validity of the Port Neighbor Information data" (page 13, paragraph "a"). As illustrated in this passage, the *Lee Provisional* discloses a flag regarding validity of information. This is completely different than "***topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database***" as recited in claim 4. While the Final Office Action argues:

> [The *Lee Provisional*] teaches a flag enabling a port. The port can either be enabled or disabled and this is indicated by a flag, this flag similar to the flag of the claim language in Claim 4 where switching entry protection flags configured with a predetermined value that determines

> whether each of the switching entries is protected from update. The argument that the Provisional fails to teach an update is moot since updating information via a port is just intended use. Intended use is not patentable material. The port as taught in the provisional shows how the port can transfer data or not based on the flag indicator of the port. One of ordinary skill in the art would see how this reads on the claim language in Claim 4 of "protection flags configured with a predetermined value that determines whether each of the switching entries is protected from update.

(FOA page 3, line 15).

Appellant respectfully disagrees. More specifically, the *Lee Provisional* does not disclose the exact same flags that could be used in a manner consistent with claim 4. To the contrary, claim 4 clearly recites "***topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database***." The switching entry protection flags include different information (*e.g.*, "a predetermined value...") than a flag that simply enables or disables a port, as disclosed in the *Lee Provisional*. Consequently, this is not just "intended use" as argued in the Final Office Action.

For at least the reason that the *Lee Provisional* fails to support a rejection under 35 U.S.C. §102, the rejection is deficient and claim 4 is allowable. As clearly illustrated above, the *Lee* provisional application fails to provide adequate support to substantiate a filing date that would permit *Lee* to be used as a 35 U.S.C. §102(e) reference in rejecting the present application. For at least this reason, claim 4 is allowable.

4. Claim 5 is Allowable Over *Lee*

The Office Action indicates that claim 5 stands rejected under 35 U.S.C. §102(e) as allegedly being anticipated by U.S. Patent Publication Number 2002/0156888 ("*Lee*"). Appellant respectfully traverses this rejection on the grounds that *Lee* does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 5 recites:

A secure data switching node comprising:

a. a plurality of physical communications ports;

b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between at least one data network node identifier and at least one of the communications ports;

c. ***a plurality of unknown destination flood control flags, corresponding to the plurality of switching entries, each of the plurality of unknown destination flood control flags configured with a predetermined value that determines whether replication of Payload Data Unit (PDU) to communication ports is prevented***; and

d. a controller implementing a secure Payload Data Unit (PDU) forwarding process, wherein implementing a secure Payload Data Unit (PDU) forwarding process includes determining, from at least one of the unknown destination flood control flags, whether replication of PDU to communication ports is prevented, the PDU forwarding process further including receiving a modification instruction including a change of at least one of the communication ports for at least one of the data network node identifiers, whereby a received PDU having as a destination data node identifier not stored in the switching database is replicated only to physical communications ports having reset unknown destination flood control flags preventing hostile data network nodes connected thereto from listening to unknown destination data traffic.

(Emphasis added).

Appellant respectfully submits that claim 5 is allowable for a least the reason that *Lee* fails to disclose, teach, or suggest a "secure data switching node comprising… ***a plurality of unknown destination flood control flags, corresponding to the plurality of switching entries, each of the plurality of unknown destination flood control flags configured with a predetermined value that determines whether replication of Payload Data Unit (PDU) to communication ports is prevented***" as recited in claim 5. First, *Lee* was filed December 21, 2001, which is after the May 25, 2001 filing date of the present application. Consequently, *Lee* is not prior art without reliance on an earlier filed provisional application.

Second, if the Office Action is attempting to rely on the April 23, 2001 filing date of the *Lee* provisional application (60/285,936), the Examiner must show that the *Lee* provisional application fully supports the claimed subject matter asserted in the rejection. Appellant respectfully submits that the *Lee Provisional* fails to provide support for at least the highlighted features of claim 5. More specifically, the *Lee Provisional* discloses "[e]ach port has a special flag indicating whether the port is 'enabled' (versus disabled) for data transfer" (page 9, last paragraph). As illustrated in this passage, the *Lee Provisional* discloses a flag that indicates whether a port is enabled for data transfer. This is completely different than "***a plurality of unknown destination flood control flags, corresponding to the plurality of switching entries, each of the plurality of unknown destination flood control flags configured with a predetermined value that determines whether replication of Payload Data Unit (PDU) to communication ports is prevented***" as recited in claim 5 for at least the reason that indicating whether a port is enabled is different than determining whether a replication of a PDU to communication ports is prevented.

For at least the reason that the *Lee Provisional* fails to support a rejection under 35 U.S.C. §102, the rejection is deficient and claim 5 is allowable. As clearly illustrated above, the *Lee* provisional application fails to provide adequate support to substantiate a filing date that would permit *Lee* to be used as a 35 U.S.C. §102(e) reference in rejecting the present application. For at least this reason, claim 5 is allowable.

5. Claim 6 is Allowable Over *Lee*

The Office Action indicates that claim 6 stands rejected under 35 U.S.C. §102(e) as allegedly being anticipated by U.S. Patent Publication Number 2002/0156888 ("*Lee*"). Appellant respectfully traverses this rejection on the grounds that *Lee* does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 6 recites:

A method of securely updating a switching database of a data switching node forwarding data traffic in a data transport network, the method comprising steps of:

a. extracting a source data network node identifier from data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network identifier as a key, the switching database including a field for indicating a predetermined value associated with the source data network node identifier configured to indicate whether a new switching entry is prevented from being added to the switching database;

c. receiving a modification instruction including a change of the communication port for the data network node identifier;

d. adding a new switching entry to the switching database if a switching entry corresponding to the source data network node identifier does not prevent entry to the switching database; and

e. ***modifying the communications port specification of a switching entry found to correspond to the extracted source data network node identifier, if a switching entry protection flag associated with the found switching entry is reset whereby preventing a redirection of data traffic processed by the data switching node***.

(Emphasis added).

Appellant respectfully submits that claim 6 is allowable for a least the reason that *Lee* fails to disclose, teach, or suggest a "method of securely updating a switching database of a data switching node forwarding data traffic in a data transport network, the method comprising steps of… ***modifying the communications port specification of a switching entry found to correspond to the extracted source data network node identifier, if a switching entry protection flag associated with the found switching entry is reset whereby preventing a redirection of data traffic processed by the data switching node***" as recited in claim 6. First, *Lee* was filed December 21, 2001, which is after the May 25, 2001 filing date of the present application. Consequently, *Lee* is not prior art without reliance on an earlier filed provisional application.

Second, if the Office Action is attempting to rely on the April 23, 2001 filing date of the *Lee* provisional application (60/285,936), the Examiner must show that the *Lee* provisional application fully supports the claimed subject matter asserted in the rejection. Appellant respectfully submits that the *Lee* provisional application fails to provide support for at least the highlighted features of claim 6. More specifically, the *Lee* provisional application discloses "[e]ach port has a special flag indicating whether the port is 'enabled' (versus disabled) for data transfer" (page 9, last paragraph). As illustrated in this passage, the *Lee* provisional application discloses a flag that indicates whether a port is enabled for data transfer. This is completely different than "***a switching entry protection flag***" as recited in claim 6.

Additionally, the *Lee* provisional application discloses "there exists a flag for each port about the validity of the Port Neighbor Information data" (page 13, paragraph "a"). As illustrated in this passage, the *Lee* provisional application discloses a flag regarding validity of information. This is completely different than "***a switching entry protection flag***" as recited in claim 6.

For at least the reason that the *Lee Provisional* fails to support a rejection under 35 U.S.C. §102, the rejection is deficient and claim 6 is allowable. As clearly illustrated above, the *Lee* provisional application fails to provide adequate support to substantiate a filing date that would permit *Lee* to be used as a 35 U.S.C. §102(e) reference in rejecting the present application. For at least this reason, claim 6 is allowable.

6. Claim 7 is Allowable Over *Lee*

The Office Action indicates that claim 7 stands rejected under 35 U.S.C. §102(e) as allegedly being anticipated by U.S. Patent Publication Number 2002/0156888 ("*Lee*"). Appellant respectfully traverses this rejection on the grounds that *Lee* does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 7 recites:

A method of securely updating data transport network topology information held in a switching database of a data switching node associated with the data transport network, the method comprising steps of:

a. extracting a source data network node identifier from data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key, the switching database including a field for indicating a predetermined value associated with ***a topology discovery disable flag configured to indicate whether switching entries are prevented from being added to the switching database***; and

c. receiving a modification instruction including a change of the communication port for the data network node identifier;

d. adding a new switching entry to the switching database if a switching entry corresponding to the source data network node identifier is not found in the switching database and the topology discovery disable flag is reset whereby a hostile data network node is prevented from connecting to the source physical communications port.

(Emphasis added).

Appellant respectfully submits that claim 7 is allowable for a least the reason that *Lee* fails to disclose, teach, or suggest a "method of securely updating data transport network topology information held in a switching database of a data switching node associated with the data transport network, the method comprising steps of… ***a topology discovery disable flag configured to indicate whether switching entries are prevented from being added to the switching database***" as recited in claim 7. First, *Lee* was filed December 21, 2001, which is after the May 25, 2001 filing date of the present application. Consequently, *Lee* is not prior art without reliance on an earlier filed provisional application.

Second, if the Office Action is attempting to rely on the April 23, 2001 filing date of the *Lee* provisional application (60/285,936), the Examiner must show that the *Lee* provisional application fully supports the claimed subject matter asserted in the rejection.

Appellant respectfully submits that the *Lee* provisional application fails to provide support for at least the highlighted features of claim 7. More specifically, the *Lee* provisional application discloses "[e]ach port has a special flag indicating whether the port is 'enabled' (versus disabled) for data transfer" (page 9, last paragraph). As illustrated in this passage, the *Lee* provisional application discloses a flag that indicates whether a port is enabled for data transfer. This is completely different than "***a topology discovery disable flag configured to indicate whether switching entries are prevented from being added to the switching database***" as recited in claim 7. Additionally, the *Lee* provisional application discloses "there exists a flag for each port about the validity of the Port Neighbor Information data" (page 13, paragraph "a"). As illustrated in this passage, the *Lee* provisional application discloses a flag regarding validity of information. This is completely different than "***a topology discovery disable flag configured to indicate whether switching entries are prevented from being added to the switching database***" as recited in claim 7 for at least the reason that indicating whether a port is enabled is different than indicating whether a switching entry is prevented from being added to a database.

For at least the reason that the *Lee Provisional* fails to support a rejection under 35 U.S.C. §102, the rejection is deficient and claim 7 is allowable. As clearly illustrated above, the *Lee* provisional application fails to provide adequate support to substantiate a filing date that would permit *Lee* to be used as a 35 U.S.C. §102(e) reference in rejecting the present application. For at least this reason, claim 7 is allowable.

7. Claim 10 is Allowable Over *Lee*

The Office Action indicates that claim 10 stands rejected under 35 U.S.C. §102(e) as allegedly being anticipated by U.S. Patent Publication Number 2002/0156888 ("*Lee*"). Appellant respectfully traverses this rejection on the grounds that *Lee* does not

disclose, teach, or suggest all of the claimed elements. More specifically, claim 10 recites:

> A secure method of forwarding data traffic having a destination unknown to a data switching node, the method comprising steps of:
>
> a. extracting a source data network node identifier from the unknown destination data traffic received on a source physical communications port of the data switching node;
>
> b. querying the switching database having a plurality of switching entries each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key, the switching database including a field for indicating a predetermined value associated with ***a global unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented***;
>
> c. receiving a modification instruction including a change of the communication port for the data network node identifier;
>
> d. replicating the received data traffic to each one of a plurality of physical communications ports of the data switching node if the global unknown destination flood control flag associated with the data switching node is reset; and
>
> e. replicating the received data traffic to each one of the plurality of physical communications ports except physical communications ports having a topology discovery disable feature set if the global unknown destination flood control flag is set whereby a hostile data network node connected to a physical communications port having the topology discovery disable flag set is prevented from spying on unknown destination data traffic.
>
> ***(Emphasis added).***

Appellant respectfully submits that claim 10 is allowable for a least the reason that *Lee* fails to disclose, teach, or suggest a "secure method of forwarding data traffic having a destination unknown to a data switching node, the method comprising steps of… ***a global unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented***" as recited in claim 10. First, *Lee* was filed December 21, 2001, which is after the May 25, 2001 filing date

of the present application. Consequently, *Lee* is not prior art without reliance on an earlier filed provisional application.

Second, if the Office Action is attempting to rely on the April 23, 2001 filing date of the *Lee* provisional application (60/285,936), the Examiner must show that the *Lee* provisional application fully supports the claimed subject matter asserted in the rejection. Appellant respectfully submits that the *Lee* provisional application fails to provide support for at least the highlighted features of claim 10. More specifically, the *Lee* provisional application discloses "[e]ach port has a special flag indicating whether the port is 'enabled' (versus disabled) for data transfer" (page 9, last paragraph). As illustrated in this passage, the *Lee* provisional application discloses a flag that indicates whether a port is enabled for data transfer. This is completely different than "***a global unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented***" as recited in claim 10 for at least the reason that determining whether a port is enabled is completely different than a global unknown destination flood control flag that indicates whether PDU replication is prevented.

Further, the only other somewhat relevant discussion in the *Lee* provisional application discloses "there exists a flag for each port about the validity of the Port Neighbor Information data" (page 13, paragraph "a"). As illustrated in this passage, the *Lee* provisional application discloses a flag regarding validity of information. This is completely different than "***a global unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented***" as recited in claim 10.

For at least the reason that the *Lee Provisional* fails to support a rejection under 35 U.S.C. §102, the rejection is deficient and claim 10 is allowable. As clearly illustrated above, the *Lee* provisional application fails to provide adequate support to substantiate a

filing date that would permit *Lee* to be used as a 35 U.S.C. §102(e) reference in rejecting the present application. For at least this reason, claim 10 is allowable.

8. Claim 13 is Allowable Over *Lee*

The Office Action indicates that claim 13 stands rejected under 35 U.S.C. §102(e) as allegedly being anticipated by U.S. Patent Publication Number 2002/0156888 ("*Lee*"). Appellant respectfully traverses this rejection on the grounds that *Lee* does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 13 recites:

> A secure method of forwarding data traffic having a destination unknown to a data switching node, the method comprising steps of:
>
> a. extracting a source data network node identifier from the unknown destination data traffic received on a source physical communications port of the data switching node;
>
> b. querying the switching database having a plurality of switching entries each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key, the switching database including a field for indicating a predetermined value associated with ***an unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented***;
>
> c. receiving a modification instruction including a change of the communication port for the data network node identifier;
>
> d. replicating the received data traffic to each one of a plurality of communications ports of the data switching node if the unknown destination flood control flags associated with the physical communications ports are reset; and
>
> d. replicating the received data traffic to each one of the plurality of physical communications ports except physical communications ports having the unknown destination flood control flag set, whereby a hostile data network node connected to a physical communications port having the associated topology discovery disable flag set is prevented from spying on unknown destination data traffic.

(Emphasis added).

Appellant respectfully submits that claim 13 is allowable for a least the reason that *Lee* fails to disclose, teach, or suggest a "secure method of forwarding data traffic having a destination unknown to a data switching node, the method comprising steps of... ***an unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented***" as recited in claim 13. First, *Lee* was filed December 21, 2001, which is after the May 25, 2001 filing date of the present application. Consequently, *Lee* is not prior art without reliance on an earlier filed provisional application.

Second, if the Office Action is attempting to rely on the April 23, 2001 filing date of the *Lee* provisional application (60/285,936), the Examiner must show that the *Lee* provisional application fully supports the claimed subject matter asserted in the rejection. Appellant respectfully submits that the *Lee* provisional application fails to provide support for at least the highlighted features of claim 13. More specifically, the *Lee* provisional application discloses "[e]ach port has a special flag indicating whether the port is 'enabled' (versus disabled) for data transfer" (page 9, last paragraph). As illustrated in this passage, the *Lee* provisional application discloses a flag that indicates whether a port is enabled for data transfer. This is completely different than "***an unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented***" as recited in claim 13 for at least the reason that determining whether a port is enabled for data transfer is different than indicating whether replication of PDU to communication ports is prevented.

Further, the only other somewhat relevant discussion in the *Lee* provisional application discloses "there exists a flag for each port about the validity of the Port Neighbor Information data" (page 13, paragraph "a"). As illustrated in this passage, the *Lee* provisional application discloses a flag regarding validity of information. This is

completely different than "***an unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented***" as recited in claim 13.

For at least the reason that the *Lee Provisional* fails to support a rejection under 35 U.S.C. §102, the rejection is deficient and claim 13 is allowable. As clearly illustrated above, the *Lee* provisional application fails to provide adequate support to substantiate a filing date that would permit *Lee* to be used as a 35 U.S.C. §102(e) reference in rejecting the present application. For at least this reason, claim 13 is allowable.

9. Claims 11 – 12 are Allowable Over *Lee*

The Office Action indicates that claims 11 – 12 stand rejected under 35 U.S.C. §102(e) as allegedly being anticipated by U.S. Patent Publication Number 2002/0156888 ("*Lee*"). Appellant respectfully traverses this rejection on the grounds that *Lee* does not disclose, teach, or suggest all of the claimed elements. More specifically, dependent claims 11 – 12 are believed to be allowable for at least the reason that these claims depend from allowable independent claim 10. *In re Fine, Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002). Appellant additionally traverses this rejection for at least the reason that *Lee* fails to meet the standards for a reference in a 35 U.S.C. §102(e) rejection.

C. Rejections Under 35 U.S.C. §103

1. Claim 2 is Allowable Over *Lee* in view of *Civanlar*

The Office Action indicates that claim 2 stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Publication Number 2002/0156888 ("*Lee*") in view of U.S. Patent Number 5,996,021 ("*Civanlar*"). Appellant respectfully traverses this rejection for at least the reason that *Lee* in view of *Civanlar* fails to disclose, teach, or

suggest all of the elements of claim 2. More specifically, dependent claim 2 is believed to be allowable for at least the reason that this claim depends from allowable independent claim 1. *In re Fine, Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002). Appellant additionally traverses this rejection for at least the reason that *Lee* fails to meet the standards for a reference in a 35 U.S.C. §102(e) rejection.

2. Claims 8 and 9 are Allowable Over *Lee* in view of *Lubarsky*

The Office Action indicates that claims 8 and 9 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Publication Number 2002/0156888 ("*Lee*") in view of U.S. Patent Number 4,893,340 ("*Lubarsky*"). Appellant respectfully traverses this rejection for at least the reason that *Lee* in view of *Lubarsky* fails to disclose, teach, or suggest all of the elements of claim 8 and 9. More specifically, dependent claims 8 and 9 are believed to be allowable for at least the reason that these claims depend from allowable independent claim 7. *In re Fine, Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002). Appellant additionally traverses this rejection for at least the reason that *Lee* fails to meet the standards for a reference in a 35 U.S.C. §102(e) rejection.

3. Claims 15 – 20 are Allowable Over *Lee* in view of *Daniell*

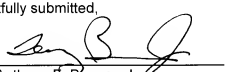
The Office Action indicates that claims 15 – 20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Publication Number 2002/0156888 ("*Lee*") in view of U.S. Patent Number 7,065,644 ("*Daniell*"). Appellant respectfully traverses this rejection for at least the reason that *Lee* in view of *Daniell* fails to disclose, teach, or suggest all of the elements of claims 15 – 20. More specifically, dependent claim 15 is believed to be allowable for at least the reason that this claim depends from

allowable independent claim 1. Dependent claim 16 is believed to be allowable for at least the reason that this claim depends from allowable independent claim 3. Dependent claim 17 is believed to be allowable for at least the reason that this claim depends from allowable independent claim 4. Dependent claim 18 is believed to be allowable for at least the reason that this claim depends from allowable independent claim 5. Dependent claim 19 is believed to be allowable for at least the reason that this claim depends from allowable independent claim 6. Dependent claim 20 is believed to be allowable for at least the reason that this claim depends from allowable independent claim 7. *In re Fine*, *Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002). Appellant additionally traverses this rejection for at least the reason that *Lee* fails to meet the standards for a reference in a 35 U.S.C. §102(e) rejection.

VIII. Conclusion

In summary, the pending claims are patentable over the applied cited art references and that the rejection of these claims should be withdrawn. Appellant therefore respectfully requests that the Board of Appeals overturn the Examiner's rejection and allow the pending claims.

Respectfully submitted,

By: 

Anthony F. Bonner, Jr.
Registration No. 55,012

Claims Appendix under 37 C.F.R. § 41.37(c)(1)(viii)

The following are the claims that are involved in this Appeal.

1. A secure data switching node comprising:

a. a plurality of communications ports;

b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between one or more data network node identifiers and one or more respective communications ports;

c. a plurality of switching entry protection flags, corresponding to the plurality of switching entries, each of the plurality of switching entry protection flags configured with a predetermined value that determines whether each of the switching entries is protected from update; and

d. a controller executing a secure switching database update process, for at least one of the switching entries, wherein executing a secure switching database update process includes determining, from at least one of the switching entry protection flags, whether the at least one of the switching entries is protected from update and receiving a modification instruction including a change of at least one of the respective communications ports for at least one of the data network node identifiers, whereby an attempt by a hostile data network node to effect a modification of the at least one communication port of a protected switching entry is prevented when the protection flag is set, enabling the data switching node to operate securely concurrently in friendly and hostile data networking environments.

2. A secure data switching node as claimed in claim 1, wherein the communication ports are represented in the switching entries via port identifiers.

3. A secure data switching node comprising:

a. a plurality of physical communications ports;

b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between one or more data network node identifiers and one or more of the respective physical communications ports;

c. a plurality of topology discovery disable flags corresponding to the plurality of switching entries, each of the plurality of topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database; and

d. a controller executing a secure data transport network topology update process for at least one of the switching entries, wherein executing a secure data transport network topology update includes determining, from at least one of the topology discovery disable flags, whether switching entries are prevented from being added to the switching database and receiving an addition instruction including a change of at least one of the respective communications ports for at least one of the data network node identifiers, whereby attempts by a hostile data network node to effect at least one addition of a switching entry specifying a communications port associated with a topology discovery disabled physical communications port are prevented, enabling the data switching node to operate securely concurrently in friendly and hostile data networking environments.

4. A secure data switching node comprising:

a. a plurality of physical communications ports;

b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port;

c. a plurality of topology discovery disable flags, corresponding to the plurality of switching entries, each of the plurality of topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database;

d. a global unknown destination flood control flag; and

e. a controller implementing a secure Payload Data Unit (PDU) forwarding process, the PDU forwarding process including a modification instruction including a change of at least one communication port for at least one of the data network node identifiers, a received PDU having a destination data node identifier not stored in the switching database is replicated only to physical communications ports having reset topology discovery disable flags preventing hostile data network nodes connected thereto from listening to unknown destination data traffic, wherein implementing a secure Payload Data Unit (PDU) forwarding process includes determining, from at least one of the topology discovery disable flags, whether switching entries are prevented from being added to the switching database.

5. A secure data switching node comprising:

a. a plurality of physical communications ports;

b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between at least one data network node identifier and at least one of the communications ports;

c. a plurality of unknown destination flood control flags, corresponding to the plurality of switching entries, each of the plurality of unknown destination flood control flags configured with a predetermined value that determines whether replication of Payload Data Unit (PDU) to communication ports is prevented; and

d. a controller implementing a secure Payload Data Unit (PDU) forwarding process, wherein implementing a secure Payload Data Unit (PDU) forwarding process includes determining, from at least one of the unknown destination flood control flags, whether replication of PDU to communication ports is prevented, the PDU forwarding process further including receiving a modification instruction including a change of at least one of the communication ports for at least one of the data network node identifiers, whereby a received PDU having as a destination data node identifier not stored in the switching database is replicated only to physical communications ports having reset unknown destination flood control flags preventing hostile data network nodes connected thereto from listening to unknown destination data traffic.

6. A method of securely updating a switching database of a data switching node forwarding data traffic in a data transport network, the method comprising steps of:

a. extracting a source data network node identifier from data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network identifier as a key, the switching database including a field for indicating a predetermined value associated with the source data network node identifier configured to indicate whether a new switching entry is prevented from being added to the switching database;

c. receiving a modification instruction including a change of the communication port for the data network node identifier;

d. adding a new switching entry to the switching database if a switching entry corresponding to the source data network node identifier does not prevent entry to the switching database; and

e. modifying the communications port specification of a switching entry found to correspond to the extracted source data network node identifier, if a switching entry protection flag associated with the found switching entry is reset whereby preventing a redirection of data traffic processed by the data switching node.

7. A method of securely updating data transport network topology information held in a switching database of a data switching node associated with the data transport network, the method comprising steps of:

a. extracting a source data network node identifier from data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key, the switching database including a field for indicating a predetermined value associated with a topology discovery disable flag configured to indicate whether switching entries are prevented from being added to the switching database; and

c. receiving a modification instruction including a change of the communication port for the data network node identifier;

d. adding a new switching entry to the switching database if a switching entry corresponding to the source data network node identifier is not found in the switching database and the topology discovery disable flag is reset whereby a hostile data network node is prevented from connecting to the source physical communications port.

8. A method as claimed in claimed in claim 7, wherein the topology discovery disable flag is associated with the source communications port.

9. A method as claimed in claimed in claim 7, wherein the topology discovery disable flag is associated with all physical communications ports of the data switching node.

10. A secure method of forwarding data traffic having a destination unknown to a data switching node, the method comprising steps of:

a. extracting a source data network node identifier from the unknown destination data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key, the switching database including a field for indicating a predetermined value associated with a global unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented;

c. receiving a modification instruction including a change of the communication port for the data network node identifier;

d. replicating the received data traffic to each one of a plurality of physical communications ports of the data switching node if the global unknown destination flood control flag associated with the data switching node is reset; and

e. replicating the received data traffic to each one of the plurality of physical communications ports except physical communications ports having a topology discovery disable feature set if the global unknown destination flood control flag is set whereby a hostile data network node connected to a physical communications port having the topology discovery disable flag set is prevented from spying on unknown destination data traffic.

11. A method as claimed in claim 10, wherein replicating the unknown destination data traffic, the method further comprises a step of suppressing the replications of the data traffic to the source communications port.

12. A method as claimed in claim 10, wherein each physical communications port further includes an associated unknown destination flood control bit, the method further comprising a step of: suppressing the replication of the data traffic to communications ports having the associated unknown destination flood control bit set.

13. A secure method of forwarding data traffic having a destination unknown to a data switching node, the method comprising steps of:

a. extracting a source data network node identifier from the unknown destination data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key, the switching database including a field for indicating a predetermined value associated with an unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented;

c. receiving a modification instruction including a change of the communication port for the data network node identifier;

d. replicating the received data traffic to each one of a plurality of communications ports of the data switching node if the unknown destination flood control flags associated with the physical communications ports are reset; and

d. replicating the received data traffic to each one of the plurality of physical communications ports except physical communications ports having the unknown destination flood control flag set, whereby a hostile data network node connected to a

physical communications port having the associated topology discovery disable flag set is prevented from spying on unknown destination data traffic.

14. A method as claimed in claim 13, wherein replicating the unknown destination data traffic, the method further comprises a step of suppressing the replication of the data traffic to the source communications port.

15. The secure data switching node of claim 1, further comprising an alarm configured for trigger if at least one of the switching entries is protected from update.

16. The secure data switching node of claim 3, further comprising an alarm configured for trigger if switching entries are prevented from being added to the switching database.

17. The secure data switching node of claim 4, further comprising an alarm configured for trigger if switching entries are prevented from being added to the switching database.

18. The secure data switching node of claim 5, further comprising an alarm configured for trigger if replication of PDU to communication ports is prevented.

19. The method of claim 6, further comprising triggering an alarm if switching entries are prevented from being added to the switching database.

20. The method of claim 7, further comprising triggering an alarm if switching entries are prevented from being added to the switching database.

Evidence Appendix under 37 C.F.R. § 41.37(c)(1)(ix)

(None)

Related Proceedings Appendix under 37 C.F.R. § 41.37(c)(1)(x)

(None)